REMARKS

This paper is responsive to the Office Action mailed from the Patent and Trademark Office on July 27, 2004, which has a five-month statutory period set to expire December 27, 2004. A two-month extension is submitted in a petition filed herewith.

Claims 1-22 are pending in the above-identified application, and all of these claims stand rejected under 35 USC 102 as being anticipated by Experton (USP 5,995,965).

In the current paper, Claims 1-7, 17, 19 and 20 remain as filed, Claim 18 is amended, and claims 8-16 and 22 are canceled. No new matter is entered. In view of the following remarks, Applicant respectfully requests reconsideration and allowance of all pending claims.

Overview of the Invention

Applicant's Fig. 1, reproduced below, depicts a simplified Internet network 100 according to the present invention including a system server 110, a user terminal 130,131 having a smart card interface 215, and a target Internet site 120, all coupled to the Internet:

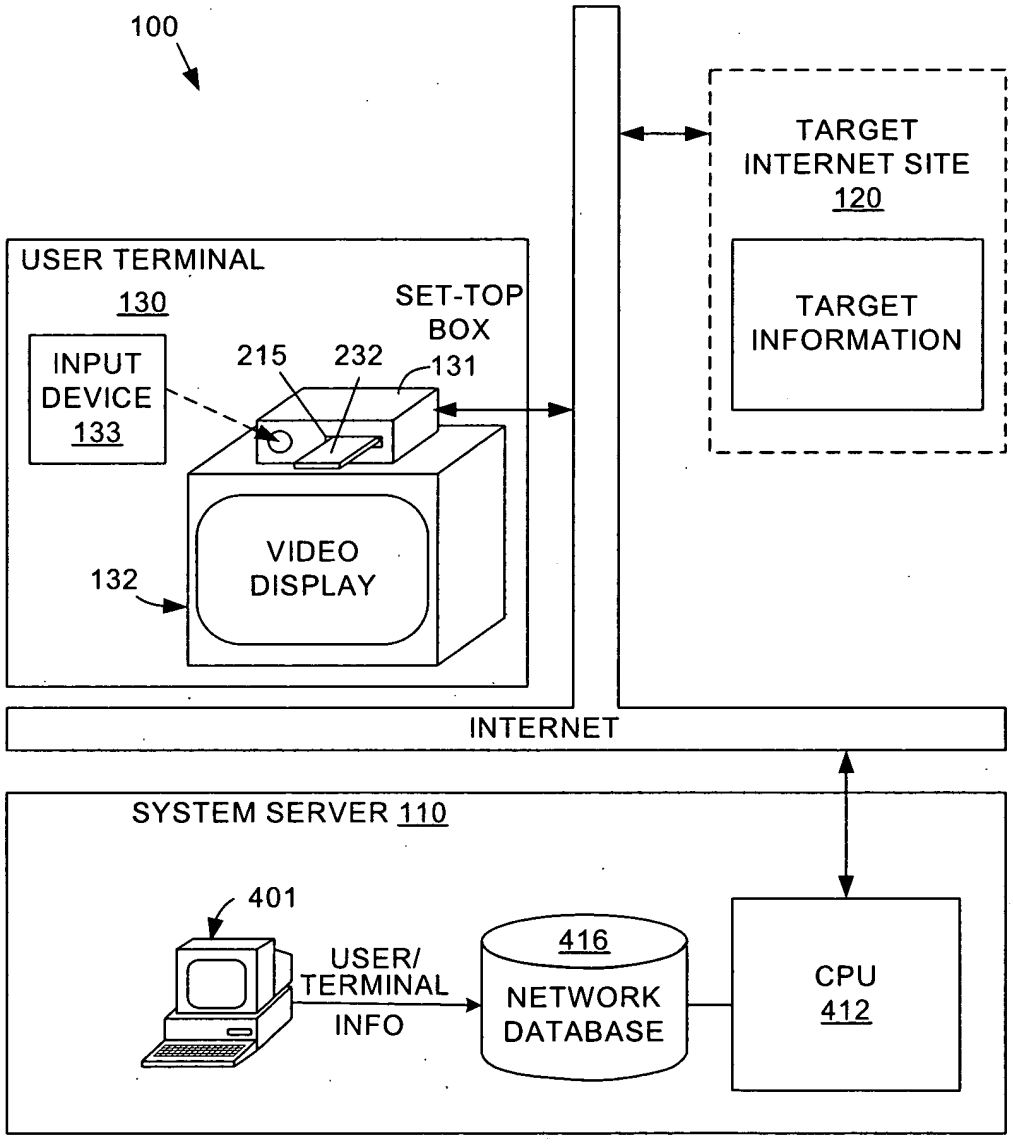

FIG. 1

System server 110 supports several authorized users. Each of the authorized users accesses the Internet using a smart card 232 through user terminal 130. System server 110 maintains a server database 416 that stores authorized user information corresponding with each of the authorized users. For example, server database 416 may store a customer number and personal ID number for each of the authorized users.

According to the invention, a user's smart card 232 is inserted into an interface 215 of user terminal 130 to initiate a process whereby user terminal 130 reads user information from smart card 232, transmits the user information to system server 110, and then, upon receiving an authorization code from system server 110, user terminal 130 uses the authorization code to retrieve a target Internet address stored in smart card 232. Finally, the retrieved target Internet address is utilized by user terminal 130 to access a target Internet site. That is, **the user terminal of the present invention is unique in that a) it requires an authorization code provided from the server to read target Internet address stored on the smart card, and b) it then uses the retrieved target Internet address to access the target Internet site.** This process is clearly shown, for example, in Applicant's Fig. 8 (reproduced below for reference), wherein user information is retrieved by user terminal 130 from a smart card and transmitted to system server 110 in block 803, and then target internet address information is retrieved from the smart card only after receiving an authorization code (blocks 808 and 809):

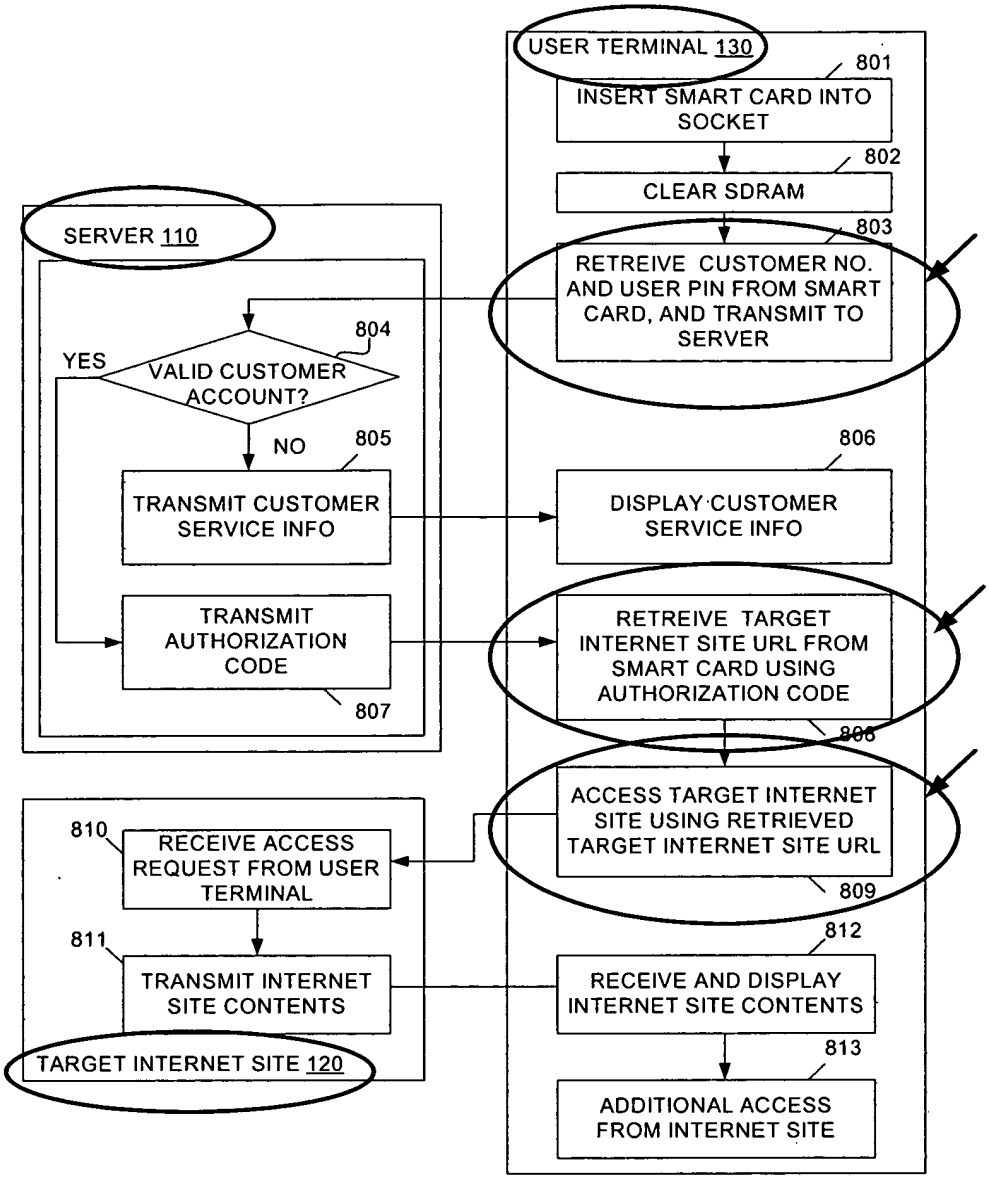

FIG. 8

Note also that the above procedure facilitates accessing an Internet site 120 that differs from system server 110--i.e., system server 110 does not need to process or control the site information transmitted from target Internet site 120 to user terminal 130. This facilitates a system whereby the owner of system server 110 can control which sites are accessed from user terminals 130 without requiring the large bandwidth necessary to support data flow to a large number of users. In such a system, the

owner can charge the target Internet site owner a fee, place the Internet site's URL on the smart card, which is then provided to the user. Thus, target Internet site information is provided to authorized users without the need for advertising the URL associated with the target information. Further, by requiring the authorization code to access the target URL, the owner of the system server prevents the owner of the target Internet site from simply creating its own smart cards to avoid payment to the owner of the system server.

Rejections under 35 USC 102

Claims 1-22 are rejected under 35 USC 102 as being anticipated by Experton (USP 5,995,965).

Claim 1 recites (in pertinent part):

> A method of accessing a target Internet site comprising:
> ...receiving an authorization code with the user terminal, the authorization code being transmitted by the server in response to the authorized user information;
> using the authorization code to retrieve a target Internet address from the smart card, wherein the target Internet address corresponds with the target Internet site; and
> using the target Internet address retrieved from the smart card to access the target Internet site.

Similarly, Claim 17 recites (in pertinent part):

> A user terminal for an Internet access network including a server and a target Internet site, the user terminal comprising:
> ...means for receiving an authorization code from the system server; and

> means for retrieving a target Internet address corresponding with the target Internet site from the smart card in response to the authorization code; and
>
> means for accessing the target Internet site in response to the retrieved target Internet address.

Claim 18 is amended to incorporate the language of Claim 22 (now cancelled), and as amended recites (similar to Claims 1 and 17):

> An Internet access network comprising:
>
> ...means for retrieving the authorized user information from the smart card within the user terminal;
>
> means for transmitting the retrieved authorized user information from the user terminal to the server;
>
> means for comparing the authorized user information transmitted from the user terminal to the server with the authorized user information stored in the server database; and
>
> means for authorizing access to the target Internet site if the authorized user information transmitted from the user terminal to the server matches authorized user information stored in the server database.

With respect to Claim 1, the above-mentioned rejection is traversed because, contrary to the Examiner's position stated on page 2 of the Office Action, Experton fails to teach or suggest "receiving an authorization code with the user terminal, the authorization code being transmitted by the server in response to the authorized user information; using the authorization code to retrieve a target Internet address from the smart card...and using the target Internet address retrieved from the smart card to access the target

Internet site", as recited in Claim 1. Instead, Experton teaches a data retrieval system whereby the user identification and "target Internet address" (i.e., patient "record sub-addresses) are read from the smart card and transmitted, and the retrieved records displayed, without the use of an authorization code (Experton, column 9, lines 27-38, copied below):

> When the processing unit senses activation of a smart card, it thus interrupts all other applications, initializes the I/O device **206**, accesses the network **400** with the address of the corresponding remote processing facility **300**, senses when two-way communication is established, passes the command signals for a data record request along with the user ID and record sub-addresses (if implemented), and receives and displays and/or prints out the retrieved data records. The commands for all of these steps may be pre-programmed into the access memory **212**, so that there is no need for any additional data entry by the user once the smart card has been activated (inserted into the reader).

Accordingly, Experton fails to anticipate the method of Claim 1.

Claims 2-7 are dependent from Claim 1, and are distinguished over Experton for at least the reasons provided above with reference to Claim 1.

Experton also fails to anticipate the user terminal of Claim 17 at least because Experton fails to teach or suggest "means for receiving an authorization code from the system server; and means for retrieving a target Internet address corresponding with the target Internet site from the smart card in response to the authorization code; and means for accessing the target Internet site in response to the retrieved target Internet address", as recited in Claim 17.

Moreover, Experton also fails to anticipate the Internet access network of amended Claim 18 at least

because Experton fails to teach or suggest "means for retrieving the authorized user information from the smart card within the user terminal; means for transmitting the retrieved authorized user information from the user terminal to the server; means for comparing the authorized user information transmitted from the user terminal to the server with the authorized user information stored in the server database; and means for authorizing access to the target Internet site if the authorized user information transmitted from the user terminal to the server matches authorized user information stored in the server database", as recited in Claim 18.

Claims 19 and 20 are dependent from Claim 18, and are distinguished over Experton for at least the reasons provided above with reference to Claim 18.

For the above reasons, Applicant requests reconsideration and withdrawal of the rejections under 35 USC 102.

CONCLUSION

Claims 1-7 and 17-20 are pending in the present Application. Reconsideration and allowance Claims 1-7 and 17-20 is respectfully requested.

Respectfully submitted,

Customer No.: 022888

Patrick T. Bever
Attorney for Applicants
Reg. No. 33,834
408-451-5902

I hereby certify that this correspondence is being deposited with the United States Postal Service as FIRST CLASS MAIL in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on December 27, 2004.

12/27/2004
Date

Signature: Rebecca A. Baumann